User Guide

McAfee Embedded Control 6.5.0

For use with Wind River Linux 5.0.1

COPYRIGHT

Copyright © 2014 McAfee, Inc., 2821 Mission College Boulevard, Santa Clara, CA 95054, 1.888.847.8766, www.intelsecurity.com

TRADEMARK ATTRIBUTIONS

Intel and the Intel logo are registered trademarks of the Intel Corporation in the US and/or other countries. McAfee and the McAfee logo, McAfee Active Protection, McAfee DeepSAFE, ePolicy Orchestrator, McAfee ePO, McAfee EMM, McAfee Evader, Foundscore, Foundstone, Global Threat Intelligence, McAfee LiveSafe, Policy Lab, McAfee QuickClean, Safe Eyes, McAfee SECURE, McAfee Shredder, SiteAdvisor, McAfee Stinger, McAfee TechMaster, McAfee Total Protection, TrustedSource, VirusScan are registered trademarks or trademarks of McAfee, Inc. or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others.

LICENSE INFORMATION

License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANY YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEBSITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

Contents

Preface **5**

About this guide 5

Audience 5

Conventions 5

Find product documentation 6

1 Introduction **7**

What is Embedded Control? 8

When to use Embedded Control? 8

Product features 9

2 Installing and configuring the software **11**

Validate the software installation 11

McAfee layer 12

Configure the project 12

Using the command-line interface 13

Using the Workbench 13

3 Getting started **15**

Enable the product 15

Configure checksum calculation 16

Verify that only authorized applications can run 17

Verify that Embedded Control tamper-proofs applications 17

Perform emergency changes 18

Index **19**

Preface

This guide provides the information you need to work with your McAfee product.

Contents

- *About this guide*
- *Find product documentation*

About this guide

This information describes the guide's target audience, the typographical conventions and icons used in this guide, and how the guide is organized.

Audience

McAfee documentation is carefully researched and written for the target audience.

The information in this guide is intended primarily for:

- **Administrators** — People who implement and enforce the company's security program.
- **Users** — People who use the computer where the software is running and can access some or all of its features.
- **Partners** — Resellers who contract with McAfee to sell McAfee products.

Conventions

This guide uses these typographical conventions and icons.

Book title, *term*, *emphasis*	Title of a book, chapter, or topic; a new term; emphasis.
Bold	Text that is strongly emphasized.
`User input, code, message`	Commands and other text that the user types; a code sample; a displayed message.
Interface text	Words from the product interface like options, menus, buttons, and dialog boxes.
Hypertext blue	A link to a topic or to an external website.

Note: Additional information, like an alternate method of accessing an option.

Tip: Suggestions and recommendations.

Important/Caution: Valuable advice to protect your computer system, software installation, network, business, or data.

Warning: Critical advice to prevent bodily harm when using a hardware product.

Find product documentation

After a product is released, information about the product is entered into the McAfee online Knowledge Center.

Task

1 Go to the **Knowledge Center** tab of the McAfee ServicePortal at http://support.mcafee.com.

2 In the **Support Content** pane:

- Click **Product Documentation** to find user documentation.
- Click **Technical Articles** to find KnowledgeBase articles.

3 Select **Do not clear my filters**.

4 Enter a product, select a version, then click **Search** to display a list of documents.

1

Introduction

McAfee® Embedded Control is a single solution that provides system integrity and change control for embedded devices. This software offers an effective way to block unauthorized applications from running on your embedded systems.

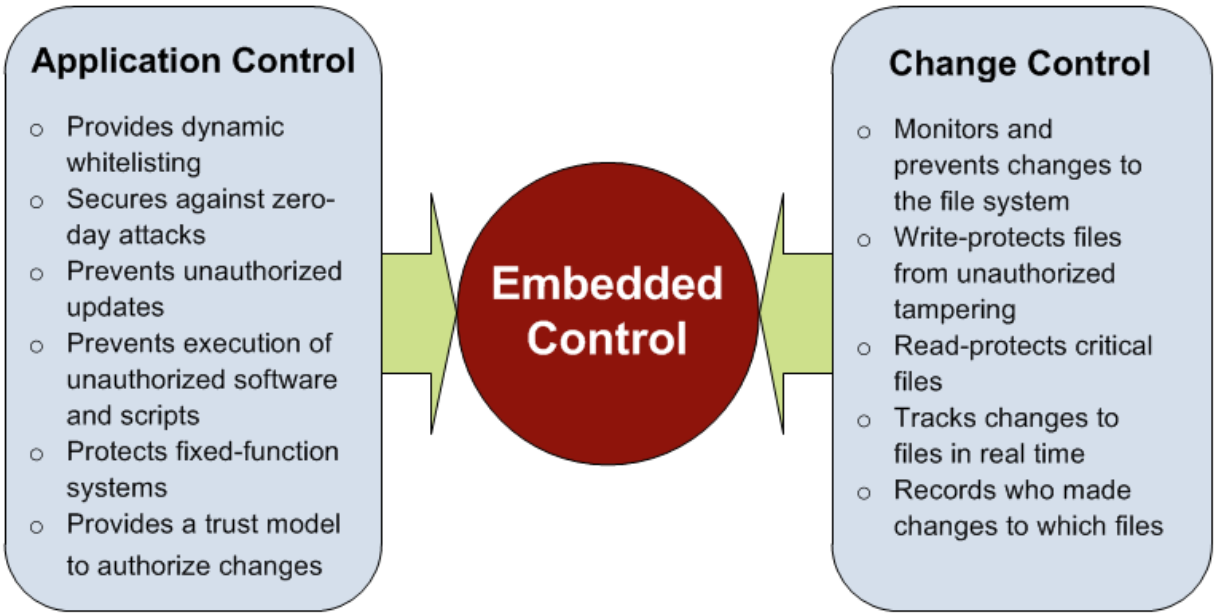
Contents

- *What is Embedded Control?*
- *When to use Embedded Control?*
- *Product features*

What is Embedded Control?

Embedded Control is a combination of McAfee Application Control and McAfee Change Control products.

When you deploy Embedded Control, the integrated features of both products are available for use. Here is a high-level overview of the features provided by these products.


Application Control
Provides dynamic whitelisting
Secures against zero-day attacks
Prevents unauthorized updates
Prevents execution of unauthorized software and scripts
Protects fixed-function systems
Provides a trust model to authorize changes
Embedded Control
Change Control
Monitors and prevents changes to the file system
Write-protects files from unauthorized tampering
Read-protects critical files
Tracks changes to files in real time
Records who made changes to which files

For detailed information about these products, see *McAfee Application Control 6.1.0 Product Guide* and *McAfee Change Control 6.1.0 Product Guide*.

When to use Embedded Control?

With the adoption of commercial operating systems in embedded devices, there are increased security risks. Embedded Control offers a one-stop security solution that enables manufacturers to use a commercial operating system without incurring risks or losing control over the systems.

This product helps you convert a system built on a commercial operating system into a black box so it works like a proprietary operating system. When you use Embedded Control on devices, it:

- Provides zero-day protection
- Minimizes security risks
- Controls what runs on your devices
- Provides real-time visibility
- Offers a deploy-and-forget solution
- Helps you to reduce support costs

This release of Embedded Control is designed to work with Wind River Linux version 5.0.1. Wind River Linux is the market-leading commercial grade Linux solution for embedded-device development. For more information about using Wind River Linux, visit the Wind River Support page or see *Wind River Linux documentation*.

Product features

Here is a description of Embedded Control features.

Execution control

Maintain system integrity by controlling what runs on your embedded devices. Embedded Control allows only authorized software to run and permits validated changes to the systems.

It automatically creates a dynamic whitelist of the authorized programs and applications. After the whitelist is created and enabled, only programs contained in the whitelist can execute. Other programs scripts and binaries (Executable and Linkable Format) that are not contained in the whitelist are considered unauthorized and prevented from executing. This prevents worms, viruses, spyware, and other malware from executing illegitimately.

System integrity

Based on your setup, Embedded Control gives you the flexibility to configure access to the protected systems. You can lock down systems to prevent even administrators from changing what is authorized to run on a system, unless presented with an authentication key.

Change tracking and control

Embedded Control detects and tracks changes in real time. It allows changes to be made only to the needed target systems and through authorized means. You can enforce change control processes by specifying authorized means of allowing changes. You can define what can be changed, such as certain files or directories, and when the changes can be applied.

Activity record and change visibility

Embedded Control records all activity for protected systems and provides visibility into the sources of change. It makes sure that only valid changes are deployed and prevents invalid changes from being deployed. The software captures detailed information for every change to a protected system, including who, what, where, when, and how. It provides an accurate, complete, and definitive record of all system changes.

Low operational expenses and overhead

Embedded Control is deployed with ease and does not have any ongoing maintenance overhead. Also, the software requires a minimal learning period and is functional across all applications immediately after activation. Embedded Control does not depend on rules or signature databases and has a small footprint.

Secure Hash Algorithm 256 (SHA256) support

With this release, we have added support for SHA256 to calculate checksum values of inventory items. SHA256 offers improved security as compared to SHA1. Although we continue to support SHA1, checksum values of inventory items will be calculated using SHA256. If you use SHA256 as the hash algorithm, we compute both SHA1 and SHA256 values while creating the whitelist. However, decision making is primarily based on SHA256 values. For more information, see *Configure checksum calculation*.

Startup script changes

With this release, the scsrvc service does not start at system restart for non-configured systems. If the software is not configured, we no longer start the Embedded Control service (scsrvc) at system start. The software is said to be *not configured* when Embedded Control is installed, software is in disabled mode, and system volume is not solidified.

2

Installing and configuring the software

Install and configure the software for the Wind River Linux target platforms.

This version of Embedded Control supports only 32-bit architecture.

Contents

- *Validate the software installation*
- *McAfee layer*
- *Configure the project*

Validate the software installation

Verify that Wind River Linux software and required licenses are installed on the system.

Task

1. Make sure that Wind River Linux 5.0.1 is installed on the development host.
   a. Navigate to `<installDir>`.
   b. Confirm that `<installDir>/wrlinux-5` and `<installDir>/wrlinux-addons` are present.
   c. Open the `<installDir>/setup.log` file and make sure that the Wind River Linux CDRs listed show 5.0.1.x.
2. Make sure that the Embedded Control software package is installed with your standard Wind River Linux installation.
   a. Navigate to the `<installDir>/wrlinux-addons/wr-idp/layers` directory.
   b. Verify that the `wr-mcafee` directory exists.
3. Validate that your license allows you to use Embedded Control.

For more information, see the *Wind River Workbench User's Guide* and *Wind River Linux 5 Getting Started Guide*.

McAfee layer

Use the McAfee layer for Wind River Linux to add Embedded Control features.

The layer framework in Wind River Linux provides modular functionality allowing you to easily add or modify features. You can add your updates as one or more layers on top of the base installation. Each layer contributes specific content without changing the base installation.

The McAfee layer (`wr-mcafee`) allows you to add the Embedded Control functionality. It is added to the standard Wind River Linux IDP installation in the `<installDir>/wrlinux-addons/wr-idp/layers` directory. After you configure the project (based on instructions in the *Configure the project* topic), the `<projDir>/layers/wr-idp/wr-mcafee` directory includes these files.

Directory	Contents	Description
conf	`layer.conf`	Layer configuration file
recipes	• `linux/linux-windriver_3.4.bbappend` • `linux/mcafee/mcafee.cfg` • `linux/mcafee/mcafee.scc`	Configuration files
	`solidcores3/files/solidcore.conf`	
	`solidcores3/solidcores3_<version>.bb`	BitBake recipe file
downloads	`solidcores3-<version>.intel-atom-baytrail.tgz`	User binary TAR file for Baytrail-based boards
	`solidcores3-<version>.intel-quark.tgz`	User binary TAR file for Quark-based boards
	`solidcores3-ksrc-<version>.tgz`	Kernel source
files	`common-licenses/McAfee`	McAfee end-user license agreement
templates	`default/README`	Read me file
	`default/image.inc`	Feature template file

Configure the project

Configure your Wind River Linux project to add Embedded Control security features to the project.

You can add Embedded Control functionality to the platform project using Wind River Workbench or command-line options on the Wind River Linux development host.

Tasks

- *Using the command-line interface* on page 13
  Add the McAfee layer to configure your project using the command-line interface (CLI).
- *Using the Workbench* on page 13
  Add the McAfee layer to configure your project using the Workbench.

Using the command-line interface

Add the McAfee layer to configure your project using the command-line interface (CLI).

Task

1 Navigate to your project directory.

These examples use <projDir> to represent the project directory. For example:

```
$ cd <installDir>/workspace/<projDir>
```

2 Set the Wind River Linux environment variables on your development host.

This command creates the `$WIND_LINUX_CONFIGURE` environment variable that appears in the examples.

```
$ <installDir>/wrenv.sh -p wrlinux-5
```

3 Configure the platform project to add Embedded Control features.

For example:

- Quark

```
$WIND_LINUX_CONFIGURE --enable-board=intel-quark --enable-kernel=standard --enabl
e-rootfs=glibc-idp --enable-addons=wr-idp
```

- Baytrail

```
$WIND_LINUX_CONFIGURE --enable-rootfs=glibc-idp --enable-kernel=standard --enabl
e-board=intel-atom-baytrail --enable-addons=wr-idp
```

In the command, the wr-mcafee layer is included by default. To exclude the layer, add the `--without-layer=wr-mcafee` option.

4 Verify that no errors are generated and the directory structure is created in the project directory.

5 Build the target file system and wait until the process is complete.

```
$ make fs
```

6 Create the image and deploy the Embedded Control-enabled platform on a target.

For more information, see the *Wind River Linux Getting Started Guide, 5*, *Wind River Linux User's Guide, 5*, and *Wind River Workbench By Example (Linux 5 Version), 3.3*.

Using the Workbench

Add the McAfee layer to configure your project using the Workbench.

Task

1 Launch Wind River Workbench, and select **File** | **New** | **Wind River Workbench Project**.

2 Select **Wind River Linux Platform Base 5.0.1** and click **Next**.

3 Select **Build Type** as **Platform** and click **Next**.

4 Type a name for the project and click **Next** to open the **Configure Options** screen.

5 Click **Advanced >>**.

6 Add the **--enable-addons** option.

   a Navigate to the **Option and Value** table.

   b Click **Add** to open the **Configure Options** dialog box.

   c Select the **--enable-addons** option.

   The selected option is displayed in the **Option** field.

   d Set the option value to **--enable-addons=wr-idp**.

   e Click **OK** to open the **Configure Options** dialog box.

7 Click **Reload** in the **Layers** pane.

8 Specify these options in the **General settings** pane.

- **Board** — Select a board. For example, **intel-quark**.
- **RootFS** — Select **glibc-idp** as the target root file system.
- **Kernel** — Select **standard**.

9 Make sure that the final configuration command is similar to:

```
$WIND_LINUX_CONFIGURE --enable-board=intel-quark --enable-kernel=standard --enabl
e-rootfs=glibc-idp --enable-addons=wr-idp --enable-parallel-pkgbuilds=4 --enable-jo
bs=4
```

10 Click **Finish** to create the project.

11 Build the target file system and wait until the process is complete.

   For detailed instructions, see *Wind River Linux Getting Started Guide, 5*, *Wind River Linux User's Guide, 5*, and *Wind River Workbench By Example (Linux 5 Version), 3.3*.

12 Create the image and deploy the Embedded Control-enabled platform on a target.

3

Getting started

After you deploy Embedded Control, enable the product to protect your device.

A few common use-cases are detailed here. For detailed information about all product features, see *McAfee Application Control 6.1.0 Product Guide* and *McAfee Change Control 6.1.0 Product Guide*.

Contents

- *Enable the product*
- *Configure checksum calculation*
- *Verify that only authorized applications can run*
- *Verify that Embedded Control tamper-proofs applications*
- *Perform emergency changes*

Enable the product

Enable the product to activate the Embedded Control software.

Before you begin

Determine the hash algorithm to use for checksum calculation in your setup.

Scenario	Description
Fresh install	For a fresh installation, SHA256 is used by default to calculate checksum values of inventory items.
Upgrade	• If you upgrade in Disabled mode, from the previous release to this release, SHA256 is used by default to calculate checksum values of inventory items. • If you upgrade in Update mode, from the previous release to this release, SHA1 is used by default to calculate checksum values of inventory items.

To change the hash algorithm used for checksum calculation, see *Configure checksum calculation*.

With this release, Application Control and Change Control licenses are shipped with Embedded Control so manual addition of license is not needed.

Task

1 Create the initial whitelist.

```
# sadmin so
```

This command creates a whitelist of all binary and script files present on the system. The whitelist controls applications and files that can run on the protected system. The time taken to create the whitelist varies from a few minutes to an hour, depending on the installed applications and system configuration.

2 Place the product in Enabled mode.

```
# sadmin enable
```

In Enabled mode, Embedded Control protects all files in the whitelist from unauthorized modification and deletion attempts. Also, Embedded Control prevents unauthorized applications or programs from running on the system.

3 Restart the McAfee Solidifier service.

```
# service scsrvc restart
```

4 Verify that the product is in Enabled mode.

```
# sadmin status
```

McAfee Solidifier status is set to **Enabled** and the volume status is set to **Solidified** for all volumes.

Configure checksum calculation

Specify whether to use SHA1 or SHA256 to calculate checksum values of inventory items.

Task

1 Determine the hash algorithm in use.

Scenario	Description
Fresh install	For a fresh installation, SHA256 is used by default to calculate checksum values of inventory items.
Upgrade	• If you upgrade in Disabled mode, from the previous release to this release, SHA256 is used by default to calculate checksum values of inventory items. • If you upgrade in Update mode, from the previous release to this release, SHA1 is used by default to calculate checksum values of inventory items.

2 Change the hash algorithm used to calculate checksum.

a Make sure the software is in Disabled mode.

```
# sadmin status
```

If the software is not in Disabled mode, type the `# sadmin disable` command and reboot the system.

b Configure checksum calculation.

```
# sadmin config set HashAlgorithm=<sha value>
```

<sha value> represents the hash function to use for checksum calculation and can be `SHA1` or `SHA256`.

If you are switching from SHA1 to SHA256, the command might take a few minutes to compute new checksum values.

c Enable the software.

```
# sadmin enable
```

d Restart the McAfee Solidifier service.

```
# service scsrvc restart
```

Verify that only authorized applications can run

On a protected system, only authorized applications or programs are allowed to run.

Task

1 Run an authorized application.

All applications that were installed before enabling Embedded Control are added to the whitelist and hence authorized. Use the `sadmin ls` command to list all whitelisted applications, then run one of them.

2 Verify that the authorized application is allowed to run.

3 Run an unauthorized application.

For example, copy an application from an external storage device, such as a USB drive to the system and try to run the application.

4 Verify that the unauthorized application is not allowed to run.

5 Review the `solidcore.log` file placed in the `/usr/local/mcafee/solidcore/log` directory.

This entry is added to the log file:

McAfee Solidifier prevented unauthorized execution of <filename> by process <processname> (Process Id: <PID>, User:<user_name>)

Verify that Embedded Control tamper-proofs applications

When Embedded Control is enabled, all files in the whitelist are protected from unauthorized modification and deletion attempts.

Task

1 Try to move or rename a binary file or application.

For example, run the following command to rename `/bin/rm.coreutils`.

```
# mv /bin/rm.coreutils /bin/myrm
```

2 Verify that the modification attempt fails.

3 Review the `solidcore.log` file placed in the `/usr/local/mcafee/solidcore/log` directory.

This entry is added to the log file:

McAfee Solidifier prevented an attempt to modify file <filename> by process <processname> (Process Id: <PID>, User:<user_name>)

Perform emergency changes

Place Embedded Control in Update mode to make emergency changes that override the protection.

Update mode opens a change window that allows you to make the needed changes. For more information about Update mode, see *McAfee Application Control 6.1.0 Product Guide*.

Task

1 Open a change window.

```
# sadmin bu
```

This command places the product in Update mode.

2 Make the required changes to the system.

3 Close the change window.

```
# sadmin eu
```

This command ends the Update mode.

Index

A

about this guide 5
Application Control 8

B

Baytrail-based boards
    configure using Workbench 13
boards
    configure using CLI 13

C

Change Control 8
change tracking 9
configuration
    using CLI 13
    using Workbench 13
conventions and icons used in this guide 5

D

directories
    installDir 11–13
    layers 11, 12
    projDir 13
    wr-mcafee 12
documentation
    audience for this guide 5
    product-specific, finding 6
    typographical conventions and icons 5
    Wind River Linux 8, 11–13

E

Embedded Control
    activate 15
    features 9
    install 11
    license 15
    supported architecture 11
    using 17
emergency changes 18
execution control 9

G

getting started 15

I

installation
    Embedded Control 11
    Wind River Linux 11

M

McAfee layer 12
McAfee ServicePortal, accessing 6
modes
    Enabled 15
    Update 18

O

operational costs 9

Q

Quark-based boards
    configure using Workbench 13

S

ServicePortal, finding product documentation 6

T

technical support, finding product information 6

V

verification
    activation 15
    installation 11
    license 11
    protection 17
    tamper proofing 17

W

whitelist
    about 9
    create 15

Wind River Linux 8
    install 11
    layer framework 12
    license 11
WIND_LINUX_CONFIGURE variable 13

Z

zero-day protection 8